DEPARTMENT OF THE NAVY
SPACE AND NAVAL WARFARE SYSTEMS COMMAND
WASHINGTON, D.C. 20363-5100

SPAWARINST 2280.2A
SPAWAR 08-2
8 May 1991

SPAWAR INSTRUCTION 2280.2A

From: Commander, Space and Naval Warfare Systems Command

Subj: PROCEDURES FOR COMMUNICATIONS SECURITY MATERIAL SYSTEM (CMS) CONTROL AND OPERATIONS OF SECURE TELEPHONE UNIT-THIRD GENERATION (STU-III) TERMINALS

Ref: (a) CMS 6
(b) EKMS-702.01, Key Management Plan, of Oct 89
(c) CMS 4L (NOTAL)
(d) SPAWARINST 5510.3H 20 Dec 88

Encl: (1) Operation of the STU-III Terminals
(2) Primary User Registration Statement
(3) General Guidance for Emergency Action Plan (EAP)
(4) Procedures for Security of Spaces and Terminals

1. Purpose. To provide additional guidance for the CMS control and operations of STU-III hardware and keying material in SPAWAR headquarters and activities.

2. Cancellation. SPAWARINST 2280.2 is cancelled.

3. Information. The STU-III, an encrypted telephone capable of providing complete security for voice and data communications, is the Navy's primary secure office communication media. The instruments have the following special features: (1) one year cryptographic period, (2) operating capability in both secure and non-secure voice modes, (3) ability to use AUTOVON or public telephone switched networks, and (4) capability to transmit data in the secure mode. This instruction addresses some of the basic capabilities and operation of the STU-III system and the responsibilities of the users.

4. Precedence. References (a) through (d) take precedence over this instruction. Discrepancies between the references and this instruction or between references must be brought expeditiously to the attention of the CMS or STU-III COMSEC Account (SCA) Custodian.

5. Policy. STU-III terminals are CMS controlled equipment and subject to annual inventory. They are to be treated as high value equipment by the users and are accountable under CMS system requirements specified in reference (a). The terminal is considered unclassified when the Crypto Ignition Key (CIK) is removed. The security of the CIK and the terminal are paramount. When the CIK is not inserted it should be safeguarded to prevent loss, unauthorized use, or tampering.

a. Each STU-III user shall:

(1) Read and abide by the entire contents of this instruction and, in particular, enclosure (1).

(2) Sign a copy of the statement provided as enclosure (1). An individual's signature signifies acceptance of responsibility for the proper handling, safeguarding, and use of the STU-III.

(3) Verify the STU-III serial number for accuracy and sign a receipt using a CMS 17 card or SF-153 form. Upon transfer, the user will inform the SCA/CMS Custodian of the change. The new user will sign for custody of the STU-III.

(4) Receive a briefing by the SCA/CMS Custodian on the operations of the specific type of STU-III terminal used.

b. Transmission and processing of data via STU-III terminals must be approved for each Automated Information System (AIS) in writing by the SPAWAR ADP Security Manager or SPAWAR activity ADP security focal point.

c. The transfer of STU-III telephone may only be effected through the SCA/CMS Custodian. No STU-III shall be removed from the building in which it is located without the knowledge and permission of the SCA/CMS Custodian.

d. Direct purchase of STU-III terminals for project/program support is <u>not</u> authorized without specific approval of the OPNAV program sponsor (OP-941J). If approved, the purchase must be coordinated with the SPAWAR CMS Custodian or field activity SCA Custodian.

6. <u>Responsibilities</u>. As a second echelon command, COMSPAWARSYSCOM has been designated Command Authority (CA) for the headquarters and activities. The CA is responsible for approving and registering SPAWAR activities' user representatives and assigning Department/Agency/Organization (DAO) code descriptions as defined in reference (b), section 6. The SPAWAR headquarters CMS Custodian (SPAWAR 08-2C) is both the designated User Representative (UR) and the CA action officer for COMSPAWARSYSCOM.

a. SPAWAR activities will use this policy for the institution of procedures to provide for proper management and security of the STU-III telephones and associated keying materials. Commanding Officers and Commanders of SPAWAR activities are directed to comply with and strictly adhere to references (a) through (d) and this instruction.

b. Responsibilities of the headquarters CMS Custodian:

(1) Principal advisor to SCA Custodian on matters related to STU-III.

(2) Provides guidance on current policy and procedures.

(3) Initial receipt and distribution of terminals.

(4) Insecurity reporting per reference (c).

(5) Resolution of CMS inconsistencies in policy.

c. Responsibilities of the headquarters User Representative:

(1) Acts as principal advisor to SCA Custodian on matters related to the keying material for STU-IIIs.

(2) Provides guidance on current policy and procedures.

(3) Submits key orders to Key Management System (KMS).

(4) Monitors status of key orders.

(5) Ensures proper application of the AIS security policy in accordance with SPAWARINST 5510.3H Chapter IX when STU-IIIs are used in the data mode.

d. Responsibilities of the SCA Custodian:

(1) Principal advisor to user on matters related to STU-III.

(2) Acts as principal advisor to user on matters related to the keying material for STU-IIIs.

(3) Inventories CIKs and keying material on a semiannual basis and STU-IIIs on an annual basis.

(4) Determines key requirements.

(5) Verifies security clearance information with the Security Office.

(6) Prepares and submits key orders to User Representative.

(7) Loading of keying material into the terminal.

(8) Storage of reserve keying material.

(9) Cognizant of the master EAP developed by SPAWAR 09H to incorporate the STU-IIIs. Enclosure (2) lists basic requirements to be incorporated into the Master EAP for the STU-III.

e. Responsibilities of the user:

(1) Installing STU-III terminal.

(2) Complies with the security, control, and accountability procedures as defined in reference (a) and this instruction. This includes entering classified material into the classified material system.

(3) Observes the terminal's two-line alphanumeric display when in the secure mode to ensure that the classification level of the call is appropriate.

(4) Controls terminal access.

(5) Maintains control of CIK.

(6) Rekeys STU-III electronically (per enclosure (1)).

(7) Reports insecurities to the SCA/CMS Custodian and the Command Security Officer, such as:

(a) Loss of terminal.

(b) Leaving the CIK in terminal when access to the terminal is uncontrolled.

(8) Supervises foreign national access to STU-IIIs.

(9) Ensures all connected AIS components are accredited for the level(s) of data processed when using the data mode.

(10) Turns in CIK to Custodian in event of transfer to another code or leaving the Command.

f. SPAWAR 09H is responsible for ensuring:

(1) Procedures described in enclosure (3) are reviewed at least annually and updated as required.

(2) Maintenance of a central listing of security clearances of SPAWAR headquarters employees to be used by the SCA Custodian when ordering keying material.

(3) Security accreditation(s) is granted for AIS when used to process data via the STU-III.

(4) Master EAP is reviewed to include emergency procedures for STU-IIIs.

g. SPAWAR 08-5 is responsible for:

(1) Installing and ensuring telephone lines are compatible with STU-III telephones.

(2) Receiving STU-IIIs and immediately notifying SCA/CMS Custodian.

7. Procedures for distribution of STU-III Materials

a. The distribution of terminals is dependent on the numbers of STU-IIIs delivered and priority established by the command for each user's need.

b. STU-III terminals will be shipped to activity supply or mail room receiving offices. These offices will not open packages but will contact the SCA/CMS Custodian for pickup. Under no circumstances will supply or mail room personnel open packages marked with controlled cryptographic items (CCI) information.

8. Operation of the STU-III terminals. The STU-III terminal has a device called a crypto ignition key (CIK) which locks and unlocks its secure mode. STU-IIIs are considered keyed only when the CIK is physically in the terminal. This allows terminals to be left unattended as long as the CIKs are removed from the terminal. STU-IIIs and CIKs are unclassified when physically separated from each other. When the CIK is inserted in the STU-III, the terminal is classified to the highest level authorized by the keying material. CIKs may be carried on your person and taken home at night. If, however, the CIK is not taken home it will be placed in a secure container. Under no circumstances will a CIK be kept in or near the users desk or terminal. The only exception to this if you are in a space cleared for open storage of secret or higher.

a. Authentication information is specified for each STU-III key ordered and is included as a part of the keying material. Each terminal's authentication information will be displayed on the distant terminal during a secure call. Authentication information includes:

(1) Classification level. During a secure call, the clearance level displayed on each terminal is the highest level common to both terminals and is the authorized level for the call.

(2) Authorization for access to Sensitive Compartmented Information (SCI) and other compartments. Specific compartments are displayed only when they are common to both terminals.

(3) Identification of the using organization (e.g., U.S. Navy). Up to three lines of specific information may be used.

(4) Foreign access to the terminal, where appropriate (e.g., US/UK, Canada).

(5) Expiration date of the terminal key.

b. Unkeyed STU-III terminals are controlled cryptographic items (CCI) which allows them to be shipped, stored and handled as other high-value office equipment; however, they are still held accountable by CMS methods as described in reference (a). User CIKs must be locally accounted for by the SCA/CMS Custodian. Loss of a CIK does not constitute a cryptographic insecurity. In case of a loss, the SCA/CMS Custodian must ensure that the serial number of the lost CIK is deleted from the terminal with which it is associated.

c. Facsimile machines. As stated in reference (a) operational doctrine permits use of the STU-III for data transmissions as long as users address data security issues. In addition, the following guidance is provided.

(1) Users must be aware that STU-IIIs protect the transmission path, but do not eliminate the need for users to provide access control to their data nor authenticate incoming data.

(2) Authority to allow unattended transmissions will be granted on a case-by-case basis determined by the local security office and SCA/CMS Custodian.

(3) Establish secure voice contact and verify that the security level displayed on the STU-III is equal to or greater than the maximum level of security of the document being transmitted, before transmitting the document.

(4) A document can only be faxed at or below the classification level indicated on the STU-III terminal message display. Faxing a document with a higher classification is a security violation. Normal procedures should then be followed for control and logging in of classified documents.

NOTE: AT&T makes a terminal which can allow unattended transmissions and receptions. It is the STU-III Access Control System (SACS) terminal. The SACS telephone contains three independent access controlling features. They can be used separately, or in any combination. This telephone allows restricted secure use of the STU-III to calls between terminals with certain keyset IDs or DAO codes loaded into them. A minimum and maximum security level for all secure calls can be set.

d. Cellular phones. They will be stored and handled as other high value equipment. Users should ensure that the terminal is secured in a manner to protect it from theft. It is recommended that the terminal be locked in the trunk of the vehicle when it is not in use or provisions for locking the terminal to the phone mount inside the car be considered. The CIK to the terminal will be kept in the possession of the user. Under no circumstances shall the CIK and the terminal be left unattended in the vehicle together. The Commander of the local activity shall determine requirements for the use of cellular phones.

e. Home phones. Reference (a) states that the terminal should be used only by the person for whom it is installed. All security requirements should be observed for preventing unauthorized access to the keyed terminal and to classified, sensitive, and for official use only U.S. Government information. The CIK shall be removed from the terminal following each use and kept away from the phone unless in use. If the terminal is used in the data mode, classified information viewed on the monitor screen should be removed as soon as possible, and not be printed unless approved storage containers are available for storage. Connections to AIS and facsimile equipment within the home must be approved by the local security office. The Commander of the local activity shall determine requirements for use of home phones after reviewing applicable directives.

f. Automated Information Systems (AIS). Operational doctrine permits use of the STU-III data port as long as users implement AIS security requirements. Per references (a) through (d), this instruction provides SPAWAR-wide policy for use of the STU-III data port.

(1) Users must be aware that STU-IIIs protect the transmission path, but do not eliminate the need for users to provide access control to their data nor authenticate incoming data.

(2) Prior to connection of a STU-III to a data device, the cognizant SPAWAR AIS security authority, (HQ organizational component ADP security officer, SPAWAR activity security officer(s), the SPAWAR HQ ADPSM, or field activity equivalent), must be consulted to verify AIS accreditation. The security accreditation must be verified for each AIS, network or computer resource to operate in accordance with Designated Approval Authority, (DAA) approved set of security requirements.

The decision to allow or disallow particular STU-III applications will be made by the responsible activity ADP security officer(s).

(3) After a STU-III application has been evaluated and approved by the activity DAA, the following requirements must be met:

(a) Authority to allow unattended transmissions will be granted on a case-by-case basis determined by the local security office.

(b) Establish secure voice contact and verify that the security level displayed on the STU-III is equal to or greater than the maximum level of security of the AIS equipment connected.

(c) AIS equipment should be connected directly to the STU-III data port.

(d) After each classified data transmission session, the SPAWAR AIS used must be sanitized to eradicate all classified data contained on internal fixed hard disk and system memory (if applicable).

NOTE: AT&T makes a terminal which can allow unattended transmissions and receptions. It is the STU-III Access Control System (SACS) terminal. The SACS telephone contains three independent access controlling features. They can be used separately, or in any combination. This telephone allows restricted secure use of the STU-III to calls between terminals with certain keyset IDs or DAO codes loaded into them. A minimum and maximum security level for all secure calls can be set.

9. Action

a. SPAWAR activities will implement the directives contained in references (a) through (d) and use the policy set forth herein as a model for overseeing the proper management and security of STU-III materials.

b. All personnel at headquarters involved with or having access to STU-III materials shall comply with all the procedures in references (a) through (d) and this instruction for the handling of STU-III material. Random unannounced inspections will be conducted by the SCA/CMS Custodian and alternates to ensure that the STU-III policies and procedures set forth herein are adhered to. Noncompliance with these policies and procedures may subject the individual to loss of access to STU-III terminals and CIKs.

R. H. AILES
Rear Admiral, U.S. Navy

Distrtibution:
(See next page)

Distribution:
SPAWAR List 5

SNDL Part 2
FKQ (ALL SPAWAR ACTIVITIES)

Stocked:
SPAWAR 08-511
(25 copies)

PRIMARY USER REGISTRATION STATEMENT

The signing of this statement constitutes an acknowledgement of the policy, responsibilities, and procedures pertinent to STU-III terminals users and an agreement to follow these procedures. This statement must be made available to all users of STU-III terminals.

POLICY

1. STU-III terminals will be used in the keyed mode as much as possible. Telephone calls can be made from most offices if all individuals occupying offices possess appropriate security clearances and visitor access is controlled.

2. STU-III terminals are considered CMS controlled equipment, subject to annual inventory by the SCA/CMS Custodian.

3. STU-III terminals and CIKs are considered UNCLASSIFIED individually, but when combined are classified to the level of the key.

4. For official use only and operations security sensitive information will be exchanged through secure modes only.

5. Transmission or processing of classified data via STU-III terminals must be approved by the SPAWAR Computer Security Manager or SPAWAR activity computer security focal point.

RESPONSIBILITIES AND PROCEDURES

1. Obtain a briefing from the SCA/CMS Custodian on terminal operation and brief all other users of the terminal using this form as a guide.

2. Include the STU-III CIK in daily lockup procedures if it is not being taken home to ensure it is not left in the telephone.

3. Ensure that the terminal is properly used and protected.

4. Observe the terminal's display during secure calls to verify the classification of the call and the identity of the other terminal.

5. Control access to the CIK during work hours and either store in an approved container or take home at night.

6. Monitor the key expiration date via the terminal's display, and electronically rekey the terminal by calling 1-800-635-6301 prior to the expiration date.

7. Report suspected insecurities to the SCA/CMS Custodian as soon as possible.

8. Notify the SCA/CMS Custodian of changes in terminal location, changes in key requirements, or any need for change in allocation of terminals.

9. Turn in CIK to Custodian in event of transfer to another code or leaving the Command.

10. Ensure that AIS equipment connected to STU-IIIs are security accredited.

Directorate/Department:__________Code:______Bldg/Room:__________

Name:__________________Signature________________________________

GENERAL GUIDANCE FOR EAPS

1. The following general guidance will assist commands in updating their EAPs.

a. Safety of personnel is paramount in any emergency. Security considerations are secondary.

b. In the event of a natural disaster (such as flooding, earthquake, or hurricane) during duty hours, the STU-III AC power cord should be disconnected.

c. If the building is being evacuated and time permits, ensure that all CIKs are removed from STU-III units and locked in a safe or that CIK control is maintained by the authorized terminal users.

d. STU-III terminal or keying material will not be removed or destroyed until directed by the proper authority.

e. SCA/CMS Custodian will ensure that extra STU-III keying material is locked in a suitable security container.

f. STU-III equipment will be considered and procedures will be provided for their handling, protection and disposition in the SPAWAR Master EAP.

PROCEDURES FOR SECURITY OF SPACES AND TERMINALS

1. The CIK must be removed whenever the user is not making a secure call. CIK may be kept in the possession of authorized users or locked in a safe or file cabinet. Normal office security is adequate to protect unkeyed STU-IIIs. The end of day security checklist must include checking all STU-III terminals to ensure that CIKs have been removed. The following security procedures apply:

a. Top Secret calls will be authorized only in SPAWAR 00H areas or other designated areas.

b. Users must know the security clearance level of coworkers and visitors if they are making a classified call on the STU-III.

c. Users must be aware of the need-to-know principle when making calls.

d. Classified calls will be stopped for periods when unauthorized individuals (i.e., vendors, maintenance personnel, cleaning personnel, etc.) are in or around the area where classified information is being discussed.

e. If possible, STU-IIIs should be placed in private/semi-controlled areas which allow privacy and prevent or curtail the unintentional disclosure of sensitive or classified data to unauthorized personnel.

f. Position STU-IIIs away from windows, doorways, and other open areas. Users must be aware that commercial phones are a major security problem when they are on or off the hook.

2. It is the terminal user's responsibility to ensure that only appropriately cleared personnel have access to classified conversations while using STU-IIIs. Traffic flow through offices may have to be modified to minimize concern of overhearing telephone conversations. A security clearance is not required for handling unkeyed terminals, but U.S. citizenship is. Personnel using the STU-III secure mode must have the appropriate clearance and need to know or be under direct supervision of such a person and have approval of the far party. The STU-III terminals will indicate on the user display the approved level of classified information that may be transmitted. In the normal telephone (unkeyed) mode classified or sensitive information will

not be passed. Prior to passing classified information in a telephone conversation, the user must be certain that the party on the other end of the conversation has the appropriate level of clearance and need to know. STU-IIIs will also be operated in combined command centers (e.g., NATO). Calls made to such sites will result in appropriate terminal displays to indicate foreign presence in the called area. All parties must ensure that the individuals in these areas are U.S. citizens with appropriate clearance and need to know. Foreign national access to STU-IIIs will only be permitted when:

a. The foreign national is visually supervised by an appropriately cleared U.S. citizen. No U.S. classified material will be disclosed to foreign nationals unless in accordance with SPAWARINST 5510.3.

b. It is clearly indicated by the supervising U.S. citizen, to the called party, prior to the start of the conversation that non-U.S. citizens are present.

3. SPAWAR headquarters and activities must ensure that procedures are in effect for control of the telephone and material during times of emergency; e.g., natural disasters, or fire. The guidelines for CCI will govern the handling of STU-IIIs. Local EAPs may be reviewed by security personnel of each facility to ensure procedures are updated to accommodate STU-III installations. Enclosure (2) lists general guidance to assist activities in updating their EAPs.

4. The following insecurities are unique to the STU-III program. Insecurities are reportable to NSA with informational copies to Director, COMSEC Material System (DCMS), CA, and UR any instance where the:

a. Authentication information displayed during a secure call is not representative of the distant terminal.

b. Display indicates that the distant terminal contains compromised key.

c. Failure of SCA/CMS Custodian to notify the KMS that a fill device listed on the conversion notice still exists in the SCA account.

d. Failure to adequately protect or to erase a CIK that is associated with a lost terminal.

5. The following occurrences are insecure practices which need not be reported unless there is an indication of espionage or sabotage (in which case reports will be forwarded to commands listed in paragraph 4 above). The following occurrences should be reported to and evaluated by SCA/CMS Custodian and Security Officer for possible follow-up action:

a. Failure to rekey a terminal within two months of the key expiration date.

b. Loss of a CIK.

c. Transmission of classified information using a terminal whose display has failed.

d. Classified conversations have been monitored or overheard by uncleared or unauthorized personnel.

e. CIK failure. If a CIK which had operated properly fails, the failure could be attributable to a malfunction in the CIK itself or in the terminal. It could also be an indication that the CIK has been copied and the copy used in the terminal. To preclude the possibility of further use in the event the CIK was copied, the failed CIK should be promptly deleted from the terminal (deleting the CIK does not affect the usability of other CIKS created for that terminal).